AMENDMENTS TO THE SPECIFICATION

Page 6, paragraph no. 4, replace with the following amended paragraph:

a third step for multiplying the derived value by a value obtained by multiplying the bit numbers per one cycle by two or more to calculate a bit number (of bit string) to be outputted from the ~~first~~ linear feedback shift register;

Page 7, paragraph no. 6, replace with the following amended paragraph:

Subsequently, the derived value is multiplied by a value obtained by multiplying the bit number per one cycle by two or more to calculate a bit number to be outputted from the ~~first~~ linear feedback shift register, a bit string corresponding to the calculated bit number is output based on the initial state value from the linear feedback shift register, and a bit is taken out from the output bit string every the number of the derived value to generate a new bit string.

Page 9, paragraph no. 2, replace with the following amended paragraph:

means for multiplying the derived value by a value obtained by multiplying the bit numbers per one cycle by two or more to calculate a bit number (of bit string) to be outputted from the ~~first~~ linear feedback shift register;

Page 10, paragraph no. 3, replace with the following amended paragraph:

Subsequently, the derived value is multiplied by a value obtained by multiplying the bit numbers corresponding to one cycle by two or more to calculate a bit number to be outputted from the ~~first~~ linear feedback shift register, a bit string corresponding to the calculated bit number is output based on the initial state value from the linear feedback shift register, and a bit is taken out from the output bit string every the number of the derived value to generate a new bit string.

Page 11, paragraph 2, replace with the following amended paragraph:

According to this invention, the linear feedback shift resistor can be divided to two resistors, i.e., the ~~first~~ linear feedback shift resistor and the second linear feedback shift resistor, which brings about enhancement of confidentiality.

Page 11, paragraph 4, replace with the following amended paragraphs:

~~means~~ a part for outputting a selectively used random number bit string having a predetermined bit number based on a secret key;

a part for outputting an amplified random number bit string having bits of a larger bit number than the selectively used random number bit string based on the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string;

a part for nonlinearly conversing the amplified random number bit string outputted from the part for outputting an amplified random number bit string to output pseudo-random numbers; and

said part for outputting a selectively used random number bit string comprising:

a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2^n)-1 per one cycle,

means for setting up an initial state value of the linear feedback shift register based on a secret key,

means for determining a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing,

means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate bit numbers to be outputted from the linear feedback shift register,

means for outputting a bit string corresponding to the bit number calculated by the above means based on the initial state value from the linear feedback shift register,

means for taking out a bit from the output bit string outputted from the above means to generate a new bit string,

means for reconstructing the linear feedback shift register such that the new bit string can be outputted from the resistor, and

means for outputting selectively used pseudo-random numbers based on the initial state value using the reconstructed linear feedback shift register reconstructed by the above means;

said part for outputting an amplified random number bit string comprising:

Page 12, second full paragraph, replace with the following amended paragraph:

~~means~~ said part (nonlinear conversion ~~means~~ part) for nonlinearly converting the amplified random number bit string comprising means for nonlinearly ~~conversing~~ converting the amplified random number bit string selected by the means for selecting ~~the~~ amplified random number bit string by a nonlinear function to output pseudo-random numbers.

Page 12, paragraph 3, replace with the following amended paragraphs:

~~According to this invention, since a selectively used random number bit string having a predetermined bit number is output based on a secret key, and a corresponding amplified random number bit string is selected from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random~~

~~number bit string, the amplified random number bit string having a larger bit number can be obtained based on the selectively used random number bit string having small bit number.~~

According to this invention, the bit string obtained by sampling, every number s, bits of a bit string whose output sequence is M sequence, when the bit number (= (2^n)-1) per one cycle of the M sequence is prime to the derived value (s), constitutes M sequence of a linear feedback shift register having other construction. Further the invention utilizes that the linear feedback shift register can be determined from the bit string having bit number of at least two cycles.

According to this invention, the pseudo-random number generator comprises the part for outputting a selectively used random number bit string having a predetermined bit number based on a secret key, the part for outputting an amplified random number bit string having bits of a larger bit number than the selectively used random number bit string based on the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string, and the part for nonlinearly converting the amplified random number bit string outputted from the part for outputting an amplified random number bit string to output pseudo-random numbers.

The part for outputting a selectively used random number bit string comprises a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2^n)-1 per one cycle, and an initial state value of the linear feedback shift register is set up based on a secret key and a derived value prime to the bit number per one cycle of the linear feedback shift register is determined based on the initial state value by means of a predetermined operation processing.

Then, the derived value is multiplied by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate bit numbers to be outputted from the linear feedback shift register, and a bit string corresponding to the bit number calculated by the above means is outputted based on the initial state value from the linear feedback shift register, and then a bit is taken out from the output bit string outputted from the above means to generate a new bit string.

Subsequently, the linear feedback shift register is reconstructed such that the new bit string can be outputted from the resistor, and selectively used pseudo-random numbers are outputted based on the initial state value using the reconstructed linear feedback shift register reconstructed by the above means.

The part for outputting an amplified random number bit string comprises a random number table in which a plurality of amplified random bit strings having a larger bit number than that of the selectively used random number bit string is beforehand stored, and a corresponding amplified random number bit string is selected from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string (i.e., the random number bit string for selection) outputted from the means for outputting selectively used random number bit string.

In the part (nonlinear conversion part) for nonlinearly converting the amplified random number bit string, the amplified random number bit string selected by the means for selecting the amplified random number bit string means is nonlinearly converted and outputted as pseudo-random numbers.

According to this method, the construction of the linear feedback shift register outputting a bit string of M sequence can be dynamically reconstructed based on the initial state value, and a new bit string of M sequence can be outputted from the reconstructed linear feedback shift register. Hence, a cryptanalysis person cannot obtain the construction of the linear feedback shift register before the reconstruction based on pseudo-random numbers outputted from the pseudo-random number generator, and cannot cryptanalyze the initial state value and secret key. As a result, high encryption strength can be obtained and confidentiality of information can be kept.

A corresponding amplified random number bit string is selected from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string, whereby the amplified random number bit string having a larger bit number can be obtained based on the selectively used random number bit string having small bit number.

Page 13, first full paragraph, replace with the following amended paragraph:

In the pseudo-random number generator of claim 7, the invention described in claim 8 is characterized in that the generator is further provided with means for generating the amplified random number bit string by a secret key given, and means for storing the amplified random bit string generated from the above means ~~the bit string~~ in the random number table~~,~~ and carrying out initial setup of the random number table.

Page 13, paragraph 3, replace with the following amended paragraph:

the means for outputting selectively used random number table are plurally provided in said part for outputting a selectively used random number bit string,

Page 13, paragraph 4, replace with the following amended paragraph:

the random number table is provided to correspond to each of the means for outputting selectively used random number table in said part for outputting an amplified random number bit string,

Page 14, first paragraph, replace with the following amended paragraph:

the means for nonlinearly converting outputs pseudo-random numbers by nonlinearly converting the amplified random number bit string selected from each of the random number tables by nonlinear function using each of the means for generating the amplified random bit string in said part for nonlinearly converting the amplified random number bit string.

Page 14, paragraph 2, replace with the following amended paragraph:

According to this invention, the selectively used random number bit string is outputted from each of the means for outputting selectively used random number bit string of the part for outputting a selectively used random number bit string, and referred to each of the random number tables using each of ~~the~~ these selectively used random number bit strings~~, and~~. Then, pseudo-random numbers ~~is output~~ are outputted by nonlinearly converting the amplified random number bit string selected from each of the random number tables through the reference by nonlinear function in the nonlinear conversion means of the nonlinear conversion part.

Therefore the throughput of the part outputting random number bit string (which constitutes a hindrance so for) on the upstream side compared with the nonlinear conversion means can be increased, which brings about enhancement of the throughput of the whole pseudo-random number generator.

Page 14, paragraph 3, replace with the following amended paragraph:

In the pseudo-random number generator of claim 9, the invention described in claim 10 is characterized in that plural random number tables are provided corresponding to each of the means for outputting selectively used random number bit string in said part for outputting an amplified random number bit string, and

~~the generator~~ which is further provided with means for subjecting each of the amplified random number bit strings selected from each of the random number tables by the means for selecting the amplified random number bit string to exclusive-or operation every the means for ~~outputting a selectively used random number bit string~~ generating the amplified random number bit string of the part for outputting a selectively used random number bit string and outputting to the nonlinear conversion means.

Page 15, first full paragraph, replace with the following amended paragraph:

In the pseudo-random number generator of claim 9 or 10, the invention described in claim 11 is characterized in that ~~the generator~~ the part for outputting an amplified random number bit string is further provided with means for replacing the random number tables with each other at a predetermined time.

Page 15, paragraph 2, replace with the following amended paragraph:

According to this invention, since the random number tables can be replaced with each other at a predetermined time in the part of outputting an amplified random number bit string, the random number tables used for the reference can be changed, which can enhance the encryption strength compared with the use of fixed random number tables.

Page 16, after paragraph 2, please add the following new paragraph:

A program to be executed by a computer for generating pseudo-random numbers of the invention described in claim 14 comprising:

Page 16, paragraph 4 which bridges over to page 17, replace with the following amended paragraph:

~~means~~ a part for outputting a selectively used random number bit string having a predetermined bit number based on a secret key;

Page 17, paragraph 4, replace with the following amended paragraphs:

~~According to this invention, since a selectively used random number bit string having a predetermined bit number is output based on a secret key, a corresponding amplified random number bit string is selected from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string, and the amplified random number bit string is nonlinearly conversed by a nonlinear function to output pseudo-random numbers, the amplified random number bit string having a larger bit number can be obtained based on the selectively used random number bit string having small bit number.~~

a part for outputting an amplified random number bit string having bits of a larger bit number than the selectively used random number bit string based on the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string; and

a part for nonlinearly converting the amplified random number bit string outputted from the part for outputting an amplified random number bit string to output pseudo-random numbers;

said part for outputting a selectively used random number bit string comprising:

a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2^n)-1 per one cycle,

means for setting up an initial state value of the linear feedback shift register based on a secret key,

means for determining a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing,

means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate bit numbers to be outputted from the linear feedback shift register,

means for outputting a bit string corresponding to the bit number calculated by the above means based on the initial state value from the linear feedback shift register,

means for taking out a bit from the output bit string outputted from the above means to generate a new bit string,

means for reconstructing the linear feedback shift register such that the new bit string can be outputted from the resistor, and

means for outputting selectively used pseudo-random numbers based on the initial state value using the reconstructed linear feedback shift register reconstructed by the above means;

said part for outputting an amplified random number bit string comprising:

a random number table in which a plurality of amplified random bit strings having larger bit number than that of the selectively used random number bit string is stored, and

means capable of selecting a corresponding amplified random number bit string from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string outputted from the means for outputting selectively used random number bit string; and

said part for nonlinearly converting the amplified random number bit string comprising means for nonlinearly converting the amplified random number bit string selected by the means for selecting the amplified random number bit string by a nonlinear function to output pseudo-random numbers.

According to this invention, the bit string obtained by sampling, every number s, bits of a bit string whose output sequence is M sequence, when the bit number (= (2^n)-1) per one cycle of the M sequence is prime to the derived value (s), constitutes M sequence of a linear feedback shift register having other construction. Further the invention utilizes that the linear feedback shift register can be determined from the bit string having a bit number of at least two cycles.

According to this invention, the pseudo-random number generator comprises the part for outputting a selectively used random number bit string having a predetermined bit number based on a secret key, the part for outputting an amplified random number bit string having bits of a larger bit number than the selectively used random number bit string based on the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string, and the part for nonlinearly converting the amplified random number bit string outputted from the part for outputting an amplified random number bit string to output pseudo-random numbers.

The part for outputting a selectively used random number bit string comprises a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2^n)-1 per one cycle, and an initial state value of the linear feedback shift register is set up based on a secret key and a derived value prime to the bit number per one cycle of the linear feedback shift register is determined based on the initial state value by means of a predetermined operation processing.

Then, the derived value is multiplied by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the linear feedback shift register, and a bit string corresponding to the bit number calculated by the above means is outputted based on the initial state value from the linear feedback shift register, and then a bit is taken out from the output bit string outputted from the above means to generate a new bit string.

Subsequently, the linear feedback shift register is reconstructed such that the new bit string can be outputted from the resistor, and selectively used pseudo-random numbers are outputted based on the initial state value using the reconstructed linear feedback shift register reconstructed by the above means.

The part for outputting an amplified random number bit string comprises a random number table in which a plurality of amplified random bit strings having larger bit number than that of the selectively used random number bit string is beforehand stored, and a corresponding amplified random number bit string is selected from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the

selectively used random number bit string (i.e., the random number bit string for selection) outputted from the means for outputting selectively used random number bit string.

In the part (nonlinear conversion part) for nonlinearly converting the amplified random number bit string, the amplified random number bit string selected by the means for selecting the amplified random number bit string means is nonlinearly converted and outputted as pseudo-random numbers.

According to this method, the construction of the linear feedback shift register outputting a bit string of M sequence can be dynamically reconstructed based on the initial state value, and a new bit string of M sequence can be outputted from the reconstructed linear feedback shift register. Hence, a cryptanalysis person cannot obtain the construction of the linear feedback shift register before the reconstruction based on pseudo-random numbers outputted from the pseudo-random number generator, and cannot cryptanalyze the initial state value and secret key. As a result, high encryption strength can be obtained and confidentiality of information can be kept.

A corresponding amplified random number bit string is selected from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string, whereby the amplified random number bit string having a larger bit number can be obtained based on the selectively used random number bit string having a small bit number.

Page 18, first full paragraph, replace with the following amended paragraph:

In program for generating pseudo-random numbers of the invention described in claim 14, the invention described in claim 15 is characterized in that the program further has, as means for functioning the program, means for generating the amplified random number bit string by a ~~secret key~~ given secret key, storing the bit string in a random number table, and carrying out initial setup of the random number table in the part for outputting an amplified random number bit string.

Page 18, paragraph 4, replace with the following amended paragraph:

the means for outputting selectively used random number table are plurally provided~~, and~~ in said part for outputting a selectively used random number bit string,

Page 18, paragraph 5, replace with the following amended paragraph:

the random number table is provided to correspond to each of the means for outputting selectively used random number table~~, and~~ in said part for outputting an amplified random number bit string,

Page 19, paragraph 1, replace with the following amended paragraph:

the means for nonlinearly conversing outputs ~~a~~ pseudo-random numbers by nonlinearly conversing the amplified random number bit string selected from each of the random number tables using each of the means for generating the amplified random number bit strings in said part for nonlinearly converting the amplified random number bit string.

Page 19, paragraph 2, replace with the following amended paragraph:

According to this invention, the selectively used random number bit string is outputted from each of the means for outputting selectively used random number bit string of the part for outputting a selectively used random number bit string, each of the random number tables is referred using each of the selectively used random number bit strings in the part for outputting an amplified random number bit string, and pseudo-random numbers are output by nonlinearly conversing the amplified random number bit string selected from each of the random number tables through the reference by nonlinear function. Therefore the throughput of the part for outputting random number bit string (which constitutes a hindrance so for) can be increased, which brings about enhancement (enhanced speed) of the throughput of the whole pseudo-random number generator.

Page 19, paragraph 4, replace with the following amended paragraph:

plural random number tables are provided every each of the means for outputting selectively used random number bit string~~, and further~~ in said part for outputting an amplified random number bit string and

Page 19, paragraph 5 which bridges over to page 20, replace with the following amended paragraph:

the program has, as means for functioning the program, means for subjecting each of the amplified random number bit strings selected from each of the random number tables by the means for selecting the amplified random bit string to exclusive-or operation every the means for outputting selectively used random number bit string of said part for outputting a selectively used random number bit string ~~and outputting to a nonlinear conversion means~~ and outputting to the

means for nonlinearly conversing of said part for nonlinearly converting the amplified random number bit string.

Page 20, paragraph 3, replace with the following amended paragraph:

According to this invention, since the random number tables can be replaced with each other at a predetermined time in part for outputting an amplified random number bit string, the random number tables used as the reference can be changed, which can enhance the encryption strength compared with the use of fixed random number tables.

Page 20, paragraph 4 which bridges over to page 21, replace with the following amended paragraph:

In program for generating pseudo-random numbers of the invention described in claim 18, the invention described in claim 19 is characterized in that the means for replacing the random number tables has function of replacing the random number tables with each other every time that the means for outputting the selectively used random number bit strings of the part for outputting a selectively used random number bit string outputs the selectively used random number bit string required for referring to each of the random number tables.

Page 21, paragraph 1, replace with the following amended paragraph:

This invention shows an example of the predetermined time in the program of claim 19. According to the invention, ~~since~~ the random number tables are replaced with each other every that the means for outputting the selectively used random number bit string outputs the selectively used random number bit string required for referring to each of the random number tables, in the part for outputting a selectively used random number bit string, the random number

tables used as the reference can be changed at short intervals, which can further enhance the encryption strength.

Page 22, fourth full paragraph, replace with the following amended paragraph:

Fig. 4 is a view schematically explaining ~~a~~ the principle of the pseudo-random number generator according to the embodiment of the present invention.

Page 22, sixth full paragraph, replace with the following amended paragraph:

Fig. 6 is a ~~conceptive~~ principle view explaining elements constructed in the random number bit string amplifying part.

Page 31, second full paragraph, replace with the following amended paragraph:

Fig. 4 is a view schematically explaining ~~function~~ a principle of a pseudo-random number generator ~~1~~ 2 according to the second embodiment of the invention. The pseudo-random number generator ~~1~~ 2 of the embodiment is a nonlinear-combiner-type pseudo-random number generator 1 materiarized by running a pseudo-random number program on computer hardware. In the embodiment, the generator is explained only in the case of using in an encryption device (see Description of the Related Art), and the explanation is omitted in the case of using in a decryption device because the explanation is similar to that in the encryption device.

Page 31, third full paragraph, replace with the following amended paragraph:

The pseudo-random number generator ~~1~~ 2 has a random number bit string outputting part 50, a random number bit string amplifying part 60, and a nonlinear conversion part ~~80~~ 70, as shown in Fig. 4. The random number bit string outputting part 50 is provided with α (the number) of means for outputting selectively used random number bit string 51. The means for outputting selectively used random number bit string 51_1 to 51_α continuously output the

selectively used random number bit string having Ni bits based on a secret key having Lk bits given by a user, and is, for example, composed of linear feedback shift register(s).

Page 33, paragraph 1, replace with the following amended paragraph:

The means 63 for processing exclusive-or par operation is constructed such that from $\alpha\beta$ of amplified random number bit strings extracted by the referring to the random number tables 62_1 to $62_{\alpha\beta}$ are subjected to the exclusive-or operation processing every the means 51 for outputting selectively used random number bit string, and the resultant α of amplified random number bit strings are output to the nonlinear conversion part ~~80~~ 70. Thereby, the amplified random number bit strings read out from the random number tables 62_1 to $62_{\alpha\beta}$ are not output to the nonlinear conversion part ~~80~~ 70 per se, but the encryption strength is prevented from depending upon the amplified random number bit string per se, and the strength is further enhanced.

Page 34, paragraph 3, replace with the following amended paragraph:

As shown in Fig. 6, the random number bit string amplifying part 60 is provided with means 67 for replacing the order of random number tables each other having a function of replacing the order of the random number tables 62_1 to $62_{\alpha\beta}$, and means 68 for generating random numbers for the replacement which generates random numbers for replacing the order used when the means 67 for replacing the order of random number tables conducts the processing for replacing the order of random number tables.

Page 34, paragraph 4 which bridges over to page 35, replace with the following amended paragraph:

The means 67 for replacing the order of random number tables gives the random numbers for the replacement generated by the means 68 for generating random numbers for the replacement as a table number to the random number tables 62_1 to $62_{\alpha\beta}$ in the generation order, and replaces the order of the random number tables based on the given random numbers, and then the order of the amplified random number bit strings within the random number table 61 is changed every the table.

Page 36, first full paragraph, replace with the following amended paragraph:

Subsequently, a principle of the method for generating pseudo-random numbers is explained by referring to Fig. 7. Fig. 7 is a flowchart explaining the method for generating pseudo-random numbers according to the embodiment of the invention.

Page 37, first full paragraph, replace with the following amended paragraph:

The setups of initial state values of the means 51 for outputting selectively used random number bit string and the random number table 61 are carried out by the above-mentioned steps S11 to S13, and thereafter they are in waiting state. When a plaintext in input to an encryption device (referring to the above-mentioned " Description of the Related Art"), which acts as trigger, the amplified processing of the random number bit string is started (steps S14 to S16). First, the selectively used random number bit strings whose each has Ni bits are outputted by the number of β by the means 51 for outputting selectively used random number bit string to store in a random number bit string amplifying part 60 (step S14).

Page 37, second full paragraph, replace with the following amended paragraph:

Subsequently, the order of the random number tables 62_1 to $62_{\alpha\beta}$ is replaced by the means ~~26~~ 67 for replacing the order of the random number tables (step S15). In this case, the number $\alpha\beta$ of random numbers for replacement are generated by the means 68 for generating random numbers for replacement, and given to each of the random number tables 62_1 to $62_{\alpha\beta}$ as table number for replacing the order of the random number tables. The table numbers are given from the random number table 62_1 to the random number table$62_{\alpha\beta}$ in the generated order.

Page 38, first full paragraph, replace with the following amended paragraph:

After completion of the processing replacing the order of the random number tables 62_1 to $62_{\alpha\beta}$, a corresponding amplified random number bit string is selected from each of the random number tables 62_1 to $62_{\alpha\beta}$ by the means 64 for selecting amplified random number bit string, whereby the processing for selecting amplified random number bit string is carried out (step S16). The means for selecting amplified random number bit string 64 refers to the corresponding random number tables 62_1 to $62_{\alpha\beta}$ using each of the random number bit strings stored within the random number bit string amplifying part 20 in the step S14, and the corresponding amplified random number bit string is selected from each of the random number tables 62_1 to $62_{\alpha\beta}$.

Page 38, third full paragraph which bridges over to page 39, replace with the following amended paragraph:

Further, these new amplified random number bit strings are output to a nonlinear conversion part ~~80~~ 70 whereby nonlinear conversion is performed. (step S18). The nonlinear conversion part ~~80~~ 70 nonlinearly converts the $\alpha\beta$ of amplified random number bit strings having

No bits to output as pseudo-random numbers of one of the amplified random number bit strings having No bits.

Page 39, first full paragraph, replace with the following amended paragraph:

When the pseudo-random numbers are outputted from the nonlinear conversion part ~~80~~ 70, the procedures from step S14 to step S18 are repeated again. Thus, pseudo-random numbers are generated to the extent required for conversing from the plaintext to ciphertext.

Page 39, second full paragraph, replace with the following amended paragraph:

According to the pseudo-random number generator ~~1~~ 2, the amplified random number bit strings having No bits lager in the bit number than Ni bits are fed to the nonlinear conversion part ~~80~~ 70 by referring to the random number tables based on the selectively used random number bit strings having No bits outputted from the means ~~51~~ 50 for outputting selectively used random number bit string. Hence, the throughput (which constitutes a hindrance so for) on the upstream side compared with the nonlinear conversion part ~~80~~ 70 can be enhanced and approximated to the throughput of the nonlinear conversion part ~~80~~ 70, which brings about enhancement of the throughput of the whole pseudo-random number generator ~~1~~ 2.

Page 39, third full paragraph which bridges over to page 40, replace with the following amended paragraph:

In response to the input of the selectively used random number bit string from the means ~~20~~ 51 for outputting selectively used random number bit string, the processing for replacing the order of random numbers is carried out. Therefore, encryption strength of the pseudo-random numbers can be enhanced. Especially, according to the embodiment of the invention, the number of combination of the random tables 62_1 to $62_{\alpha\beta}$ can be converted to that of factorial

(hereinafter "factorial" is represented by "!") of αβ. Hence, when it supposed that the random number tables 61 are known, effective attack requires calculation of (2^(αβ×Ni))×(αβ) !. The amount of the calculation is larger than the calculation amount for searching the whole number of a secret key of Lk bits, and therefore sufficiently enhanced encryption strength is given.

Page 40, first full paragraph, replace with the following amended paragraph:

Further, in the above-mentioned pseudo-random number generator ~~1~~ 2, by referring to plural (β) of random number tables using the random number bit strings outputted from the means 51 for outputting selectively used random number bit string, the random number bit string selected from each of the random number tables are subjected to the exclusive-or processing. Hence, it is prevented that encryption strength depend on the means 66 for generating amplified random number bit string per se as the case that the amplified random number bit strings read out from the random number table part 61 are output per se to the nonlinear conversion part 80, and encryption strength is further enhanced.

Page 40, second full paragraph, replace with the following amended paragraph:

Subsequently, one example according to the embodiment of the invention is explained. Fig. 8 is a conceptive view schematically showing pseudo-random number generator ~~1~~ 2 of the example. Fig. 9 is a conceptive view schematically showing the random number table 61. In the example, each setting value (parameter) is set in the following manner.

Page 41, paragraph 2, replace with the following amended paragraph:

The nonlinear function f(x) of the nonlinear conversion part ~~80~~ 70:

Page 43, paragraph 1, replace with the following amended paragraph:

In this example, the means 51 for outputting selectively used random number bit string reconstructs the linear feedback shift register 53 based on the secret key given by a user, and outputs the random number bit string using the reconstructed linear feedback shift register ~~53'~~ 53.

Page 43, paragraph 2, replace with the following amended paragraph:

First, the construction and operation of the means 51 for outputting selectively used random number bit string are explained. The means 51 for outputting selectively used random number bit string is provided with the means ~~12~~ 52 for setting initial state value, the linear feedback shift register 53 and the means ~~14~~ 54 for reconstructing linear feedback shift register, as shown in Fig. 8.

Page 43, paragraph 3, replace with the following amended paragraph:

The means ~~12~~ 52 for setting the initial state value, which sets up an initial state value based the secret key given by a user, converts the secret key K to a bit string, and assigns it as an initial state value into the inside of the shift register of the linear feedback shift register 53. In this example, as the means ~~12~~ 52 for setting initial state value, RC4 Syppetric Streap Cipher (available from RSA Data Security Inc.) is used, and it is shared with the means 66 for generating amplified random number bit string.

Page 43, paragraph 4, replace with the following amended paragraph:

The linear feedback shift register 53 has n of shift registers storing information of one bit and an exclusive-or operation circuit, similarly to one explained in the above-mentioned "Description of the Related Art". Further, in this embodiment, the register 53 is set beforehand

to the construction capable of outputting a bit string having bit number m of (2^n)-1 per one cycle, what is called M sequence.

Page 44, first full paragraph, replace with the following amended paragraph:

The means ~~14~~ 54 for reconstructing linear feedback shift register has a function of reconstructing the linear feedback shift register 53 by dynamically changing its construction by the secret key K. For example, a bit string obtained by sampling, every the number s, bits of a bit string whose output sequence is M sequence, when the bit number (= (2^n)-1) per one cycle of the M sequence is prime to the derived value (s) (i.e., they do not have divisors other than 1), constitutes M sequence of a linear feedback shift register having other construction. Further, the reconstruction of the linear feedback shift register 53 is carried out by utilizing that the characteristic polynomial of the linear feedback shift register, which is capable of outputting the bit string and has equivalent and minimum construction, can be obtained from the bit string having bit number of at least two cycles by means of Berlekamp-Massay algorithm.

Page 44, second full paragraph, replace with the following amended paragraph:

In the means ~~14~~ 54 for reconstructing linear feedback shift register, the derived value s is calculated from the initial state values given by the initial state value setting part ~~12~~ 52, the derived value s is multiplied by a value 2m obtained by multiplying the bit number m (= (2^n)-1) corresponding to one cycle of the linear feedback shift register 53, and the bit number 2ms of the bit string to be outputted from the linear feedback shift register 53 is calculated.

Page 45, fourth full paragraph which bridges over to page 46, replace with the following amended paragraph:

Fig. 12 is a flow chart for explaining the reconstruction processing of the linear feedback shift register 53. First, the initial state value is set by the means ~~12~~ 52 for setting the initial state value (step S41). The initial state value is set based on the secret key K of Lk bit given by a user. When the initial state value is set by the secret key in the means ~~12~~ 52 for setting the initial state value, the initial state value is set within the shift register of the linear feedback shift register 53.

Page 47, second full paragraph, replace with the following amended paragraph:

The reconstructed linear feedback shift register ~~53'~~ 53 has a characteristic polynomial having the same order as the register before the reconstruction and having the connection different from the register before the reconstruction. Thus, the reconstructed linear feedback shift register has a construction capable of outputting N sequence different from the register before the reconstruction, if the same initial state value as the register before the reconstruction is given to the reconstructed linear feedback shift register.

Page 47, third full paragraph which bridges over to page 48, replace with the following amended paragraph:

After the reconstruction of the linear feedback shift register 53 is completed by means 14 for reconstructing the linear feedback shift register, a random number bit string for the selection is generated based on the initial state value from the reconstructed linear feedback shift register ~~53'~~ 53 (step S47). Thereby, the random number bit string for the selection of M sequence different from that before the reconstruction is generated from the random number generating part 50.

Page 48, third full paragraph, replace with the following amended paragraph:

Subsequently, the method for generating pseudo-random numbers using the pseudo-random number generator ~~1~~ 2 provided with the means 51 for outputting selectively used random number bit string is explained. Fig. 10 is a flowchart explaining the method for generating pseudo-random numbers according to the embodiment of the invention.

Page 49, first full paragraph, replace with the following amended paragraph:

Then, the linear feedback shift register 53 is reconstructed based on the initial state value (step S22), and an initial state value of the reconstructed linear feedback shift register ~~53'~~ 53 is set up (step S23). The setup of the initial state value is performed in the respect to all the means for outputting random number bit string 11_1 to 11_8.

Page 49, second full paragraph, replace with the following amended paragraph:

Subsequently, a random number bit string outputting part 60 conducts an initial setup of a random number table 61 (step S24). In this case, the secret key K is first given to means 66 for generating amplified random number bit string and the processing of generating a random bit string is carried out at high speed. In this example, since the means 66 for generating amplified random number bit string is shared with the means for setting initial state value ~~12~~ 52 of the means ~~51~~ 51_1 to 51_8 for outputting selectively used random number bit string, as mentioned above, the random bit string output as the initial state value from the linear feedback shift register 53 is used as it is, without outputting the bit string separately.

Page 51, fourth full paragraph which bridges over to page 52, replace with the following amended paragraph:

Subsequently, after the same processing as described above is carried out for the random number tables 62_3 to 62_{16} (Yes in the step S30) whereby a total of eight new amplified random number bit strings are generated, they are outputted to the nonlinear conversion part ~~80~~ 70 and transferred to the nonlinear conversion stage.

Page 52, first full paragraph, replace with the following amended paragraph:

In the nonlinear conversion part ~~80~~ 70, input of the eight new amplified random number bit strings having No bits from the random number bit string amplifying part 60 brings about nonlinear conversion of the bit strings by the nonlinear function f(x) (step S34) to give one random number bit string having 16 bits. Then, the processing of the steps S25 to S34 are repeatedly performed whereby a required number of pseudo-random numbers are obtained.

Page 52, fourth full paragraph which bridges over to page 53, replace with the following amended paragraph:

Fig. 13 is a table showing the result obtained by measuring the throughput. The conventional type in the Table is the nonlinear-combiner-type pseudo-random number generator as shown in Fig. 17 which is composed of eight of linear feedback shift registers (LFSR) 53 and a nonlinear conversion part ~~80~~ 70.

Page 53, paragraph 1, replace with the following amended paragraph:

According to the experimental result, a mean throughput of the pseudo-random number generator ~~1~~ 2 is enhanced from a mean throughput of the linear feedback shift registers 53 as it is to that of nonlinear conversion part 80, and the enhanced throughput is about 170 times (i.e.,

116.4Mbps/sec ÷ 0.680Mbps/sec = 171.176----) that of the conventional type. Hence, the throughput result shows that the use of the random number table 62 is effective to enhance processing speed of the pseudo-random number generator ~~1~~ 2.

Page 53, paragraph 2, replace with the following amended paragraph:

The throughput of the pseudo-random number generator ~~1~~ 2 used in the example is represented the following formula:

Page 53, paragraph 3, replace with the following amended paragraph:

In the formula (1), T1 represents a mean throughput of one linear feedback shift registers 53, T2 represents a mean throughput of RC4 (means 66 for generating amplified random number bit string), T3 represents a mean throughput of the processing for replacing random number tables by the means 67 for replacing the order of random number tables, T4 represents a mean throughput of one random number table, and T5 represents a mean throughput of the nonlinear conversion part ~~80~~ 70. On the assumption that the calculated amount of the random number table 62 can be neglected from the formula (1), the throughput of the pseudo-random number generator 1 can be brought close to that of the nonlinear conversion part ~~80~~ 70 with reduction of a ratio (No bits/Ni bits), whereby the processing can be further enhanced.

Page 54, paragraph 1, replace with the following amended paragraph:

In contrast, the encryption strength of pseudo-random numbers is verified using a tool for verifying pseudo-random numbers of NIST (general name). The NIST is a tool for performing a test of randomness on physical random numbers and output data from a pseudo-random number generator, and also a statistical package including 16 tests. The NIST is explained in detail in "http://crsc.nist.gov/rug". Fig. 14 is a table showing parameter of NIST used in the verification.

When p-value outputted by conducting the various tests satisfies the condition of 0<p-value<1, it is considered that the corresponding tests are passed. The pseudo-random numbers of the pseudo-random number generator ~~1~~ 2 according to this example was verified, and consequently it was confirmed that all the tests were passed. Fig. 15 is a view showing the verified result of NIST in this experiment.